

**Chief Information Officers Section
Office of the Governor
State of Utah**

June 20, 2002

HIPAA and Related Security Requirements Work Group

Purpose

The CIO has formed this work group at the suggestion of the Chief Technical Architect. ITS is providing staff and research support for the members of the work group. The work group has been tasked to accomplish the following objectives:

- a. Identify all agency stakeholders with HIPAA and related security requirements.
- b. Establish a commonly agreed upon security requirements set for HIPAA and all other agencies with encryption, data security, and logging requirements.
- c. Identify gaps in terms of technology and policy to meet identified common agency security requirements.
- d. Identify security policy additions and changes that must be in place to support agency requirements.
- e. Prepare necessary security policy documents, for approval by SISC and the ITPSC.
- f. Identify alternative technology solutions for meeting the security requirements.
- g. Complete a financial impact assessment for each alternative solution.
- h. Review with federal stakeholders policy and technology recommendations and solicit comment where practicable.
- i. Recommend to the CIO and ITS a best-case, and where practicable, a least cost solution, for meeting all of the identified agency requirements.
- j. Establish firm timelines and deliverables for any IT projects required to implement the recommendations of the workgroup.

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), enacted on August 21, 1996 as Public Law 104-191, authorized the Secretary of Health and Human Services (HHS) to develop security standards to prevent inadvertent or intentional unauthorized use or disclosure of any health information that is electronically maintained or used in an electronic transmission. This law affects several titles in the United States Code.

HIPAA has immediate implications for security policy development as well as appropriate infrastructure provisioning to meet basic requirements. It has been suggested by a number of groups actively working on HIPAA policy development that a minimum of 19 specific security policies will need to be addressed to meet the ultimate HIPAA security rule requirements. In light of these specific requirements, it was also determined that existing State security policies will need to be reviewed and modified. This does not address the related procedural and infrastructure issues that will need to be associated with that policy development.

In order to meet HIPAA compliance requirements, a workgroup has been formed, which consists of key members of the Information Technology Service (ITS) group and selected agency personnel. The purpose of this new workgroup is to collect and analyze departmental security and encryption requirements in order to determine if a single policy and infrastructure implementation, that is sufficiently restrictive, will meet agency needs.

Agency Common Requirements

Each agency represented in the work group have submitted security requirements from federal agencies such as Health and Human Services (HIPAA), Criminal Justice/FBI (CJIS), Public Safety, Internal Revenue Service and others. The work group has analyzed these requirements with ITS staff assistance resulting in the following list of common requirements, which if met by the state, will ensure security compliance with rules and regulations promulgated by these agencies:

Access Control: Access control mechanisms must be employed across all State of Utah networks to ensure a given user has been granted the permission to access a system resource in the manner authorized.

Advanced Authentication: Advanced authentication should be used in cases where un-trusted inbound traffic (with the exception of Internet mail and push broadcasts) is accessing the trusted State of Utah network. Authentication of the unique user identity can be a unique encrypted logon and password combination and/or use of other authentication methods including but not limited to biometrics, smart cards, tokens, digital signatures (such as VeriSign), etc.

Audit Trails: For any State of Utah operated network, functionality should be added for real-time monitoring of networked and host-based systems to detect security vulnerabilities and incidents. The minimum amount of information to be captured in an audit record is:

1. The identity of each user and, where possible, the device having access to the system or attempting to access the system.
2. The time and date of the access (synchronized with an atomic clock to the nearest 1/10 of a second), time and date of log off.
3. Any activities which might modify, bypass or negate security safeguards controlled by the computer system.

Authorization: Once authenticated, users must be granted only specific access to the system's resources that they require to perform their duties.

Encryption: To prevent unauthorized disclosure of sensitive and valuable information, all host access to restricted information to/from the state trusted network from un-trusted networks must be encrypted with no less than 128 bit encryption. Examples of encryption mechanisms that provide 128 bit or better encryption are Secured Socket Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Advanced Encryption Standard (AES), RSA (Rivest, Shamir & Aldeman) Elliptic Curve Cryptography (ECC), etc...

Firewalls: Prior to the deployment of every State of Utah firewall, a diagram of permissible paths with a justification for each access path must be submitted to ITS. Change control will be used to document all changes. Permission to enable any paths will be granted by the agency security manager only when (1) the paths are necessary for important business reasons, and (2) adequate security measures will be used. Any state computer/data resource that exists on the trusted network must be firewalled from external (un-trusted) traffic with the exception of production services designed to be homed in a demilitarized environment (http, internet mail), or where stateful packet inspection is not required. At a minimum, traffic filter firewalls should have

the ability to screen and log traffic at the network and transport protocol layers. Firewall implementations should provide the capability to screen traffic at the network and transport layers. Likewise, every network connectivity path not specifically permitted must be denied by firewalls.

Identification: Each individual who is authorized to access sensitive/restrictive information must be uniquely identified.

Intrusion Detection: State of Utah locations with hosts containing sensitive /restricted information must include intrusion detection systems. These intrusion detection systems must each be configured according to the specifications defined by ITS security in cooperation with agencies. Intrusion detection systems must notify technical staff in a position to take corrective action. In addition, all State of Utah locations must incorporate virus protection and removal software.

Logging: All transactions with sensitive/restrictive information originating from State of Utah networks or access devices must be logged. Furthermore, all suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged and reported to ITS Security. The integrity of these logs must be protected. These logs must be promptly removed from the recording systems and stored in a physically protected container for up to 7 years. Access methods to retrieve information from the logs must be provided, and, the logs must be reviewed periodically to ensure that the security standards are being met. All logs shall be considered protected information in terms of GRAMA.

Physical Security: Information retrieved from trusted network resources must be secured from unauthorized persons.

System Design Documentation: Any entity using sensitive/restricted info must develop and maintain written documentation of the overall design and security features of their system.

Vulnerability Patching: Apply fixes or measures to stop the exploitation of known vulnerabilities.